AO 91 (Rev. 11/11) Criminal Complaint

UNITED STATES DISTRICT COURT

for the

District of New Jersey

United States of America
v.
Arushobike Mitra and Garbita Mitra

Case No. 20-mj-13309 (LDW)

Defendant(s)

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of May 2019 to November 2019 in the county of Hudson in the _____ District of New Jersey, the defendant(s) violated:

Code Section	*Description of Offenses*
See Attachment A	

This criminal complaint is based on these facts:

See Attachment B.

☑ Continued on the attached sheet.

/s/ Brendon Murray
Complainant's signature

Brendon Murray, Special Agent
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone *(specify reliable electronic means)*.

Date: 06/10/2020

/s/ Leda Dunn Wettre
Judge's signature

City and state: District of New Jersey

Hon. Leda Dunn Wettre, U.S. Magistrate Judge
Printed name and title

Print Save As... Attach Reset

ATTACHMENT A

Count One – Wire Fraud Conspiracy

From in or about May 2019 through in or about November 2019, in the District of New Jersey and elsewhere, defendants ARUSHOBIKE MITRA and GARBITA MITRA, along with other co-conspirators known and unknown, did knowingly and intentionally conspire and agree with each other and others to devise a scheme and artifice to defraud elderly victims, and to obtain money and property from the elderly victims thereof by means of materially false and fraudulent pretenses, representations, and promises, and, for the purpose of executing such scheme and artifice to defraud, did transmit and cause to be transmitted by means of wire communications in interstate and foreign commerce, certain writings, signs, signals, pictures, and sounds, contrary to Title 18, United States Code, Section 1343.

In violation of Title 18, United States Code, Section 1349.

Count Two – Mail Fraud Conspiracy

From in or about May 2019 through in or about November 2019, in the District of New Jersey and elsewhere, defendants ARUSHOBIKE MITRA and GARBITA MITRA, along with other co-conspirators known and unknown, did knowingly and intentionally conspire and agree with each other and others to devise a scheme and artifice to defraud solicited persons, and to obtain money and property from them by means of materially false and fraudulent pretenses, representations, and promises, and, for the purpose of executing such scheme and artifice to defraud, did knowingly cause to be placed in any post office or authorized depository for mail any matter or thing to be sent or delivered by the Postal Service and/or Commercial Mail Delivery Service, contrary to Title 18, United States Code, Section 1341.

In violation of Title 18, United States Code, Section 1349.

ATTACHMENT B

I, Brendon Murray, a Special Agent with the Social Security Administration, Office of the Inspector General, have knowledge of the following facts based upon both my investigation, a review of reports, and discussions with other law enforcement personnel and others. Because this Complaint is being submitted for the limited purpose of establishing probable cause, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts which I believe are necessary to establish probable cause. Unless specifically indicated, all conversations and statements described in this affidavit are related in substance and in part. Where I assert that an event took place on a particular date, I am asserting that it took place on or about the date alleged.

At all times relevant to this complaint:

BACKGROUND

1. The Department of Homeland Security ("DHS") / HSI, United States Postal Inspections Service ("USPIS"), Social Security Administration ("SSA"), Office of the Inspector General ("OIG"), and other agencies are investigating multiple criminal schemes perpetrated by individuals operating one or more call centers believed to be in India, who impersonate U.S. government officials, including SSA, and well-known businesses by "spoofing" legitimate phone numbers and sending recorded messages that are transmitted across the Internet to the phones of American consumers. These robocalls purport to be from federal government agencies, elements of foreign governments, and/or legitimate businesses, conveying alarming messages, such as: the consumer's Social Security number or other personal information has been compromised or otherwise connected to criminal activity; the consumer faces imminent arrest; their assets are being frozen; their bank and credit accounts have suspect activity; their benefits are being stopped; they face imminent deportation; or combinations of these things—all lies intended to induce consumers to speak to the fraudsters. When consumers answer the calls or return voicemail messages, the fraudsters offer to "resolve" these legal matters by immediate transfers of funds to settle the purported legal obligation, or to hold the consumer's assets only temporarily while the crisis resolves. In reality, the consumer is neither under investigation nor in legal jeopardy, and the same threatening robocall was made simultaneously to thousands of other U.S. consumers.

2. Investigation has revealed that from October 2018 to September 2019, the SSA alone received more than 465,000 complaints from U.S. consumers about callers impersonating SSA officials. Consumer losses associated with these complaints exceed $14 million. Similarly, the Federal Trade Commission ("FTC") estimates that more than 76,000 U.S. consumers filed complaints about fraudulent SSA impersonations, with estimated consumer losses reaching approximately $19 million between April 2018 and March 2019.

3. A second common technique used by the perpetrators involves refund fraud and remote computer access in which the unknown subject(s) gain remote access to the victims' computer. The scheme often consists of either a pop-up window on the victim's computer displaying a phone number to call for "Internet technical support services"; or the victim receives a telemarketing call informing the victim that their previously purchased anti-virus software is not up to date. The victim is then compelled to call the number displayed on the screen and/or follow the instructions of the tech support representative. Upon doing so, the victim is told that the anti-virus and/or protection he/she previously purchased was not sufficient for the victim's computer and, as a result, he/she is entitled to a refund. The unknown caller then states that the refund can be issued via wire into the victim's bank account. The victim is coerced into providing the unknown caller with remote access to his/her computer and the unknown perpetrators are able to move United States currency ("USC") from one of the victim's financial accounts to the victim's checking account, thus reflecting a significantly higher balance. As result of the transfer, the unknown caller advises the victim he/she was mistakenly overpaid and convinces the victim that he/she needs to send the money back via wire transfer and/or cash in the mail.

4. During March 2019, the Foundation for Worldwide International Student Exchange ("WISE") received information concerning participants in the Omni Orlando Championgate (OMNI) Student and Exchange Visitor Program (SEVIS) being involved in fraudulent activity. The students had obtained J-1 classification visas through the U.S. Department of State ("DSS") in coordination with US Citizenship and Immigration Services ("USCIS"). The purpose of the visas was to participate in programs for teaching, instructing or lecturing, studying, observing, conducting research, consulting, demonstrating special skills, receiving training, or to receive graduate medical education or training. OMNI served as a host organization / sponsor in the hospitality and tourism industry. According to the information provided to WISE, an exchange visitor reported that there was a suspected bank fraud scheme involving participant students. The exchange visitor explained that the scam involved students being recruited by "dealers" to open multiple bank accounts with different financial institutions. The accounts were then used to receive

large wire transfers and the money was withdrawn by the students in the United States and provided to the "dealers" to be returned to India. Each participating student received a percentage of the money transfer. The exchange visitor further alleged that those participating in the fraud primarily originated from the Kolkata campus of International Institute of Hotel Management ("IIHM") University in India.

5. According to SSA records, defendants ARUSHOBIKE MITRA, GARBITA MITRA, Co-Conspirator 1 (hereinafter "CC1"), and Co-Conspirator 2 (hereinafter "CC2"), presented Certificates of Eligibility for Exchange Visitor (J-1) Status, Form DS-2019s, to the SSA in order to secure their social security account numbers. The Form DS-2019s authorized defendants ARUSHOBIKE MITRA, GARBITA MITRA, CC1, and CC2 to be lawfully present in the United States as Student Interns.

6. During June 2018, defendants ARUSHOBIKE MITRA and GARBITA MITRA completed Applications for Original Social Security Numbers, Form SS-5s, and both provided SSA with the same mailing address and telephone number: specifically, 8220 Matisee Street, Apt. 5316, Championsgate, Florida 33896 and (321)333-2176. Additionally, defendants ARUSHOBIKE MITRA and GARBITA MITRA both presented sponsor letters from OMNI confirming their participation in the SEVIS program.

THE SCHEME TO DEFRAUD

7. On or about November 19, 2019, law enforcement officers from the Hoboken Police Department ("HPD"), Hoboken, NJ, responded to the FedEx store located at 119 River Road, Hoboken, NJ ("Hoboken FedEx Store"), based on a report of a suspicious package. The suspicious package, identified by FedEx tracking number 778058884441, was addressed to FedEx and was shipped by an individual identified as VICTIM 1 of Mccammon, Idaho. The suspicious package was not claimed at the Hoboken FedEx Store. Consequently, Hoboken FedEx Store management opened the package and observed a glass jar wrapped in plastic that was filled with envelopes wrapped in aluminum foil. The envelopes were found to contain United States Currency ("USC"). The Hoboken FedEx Store management immediately contacted the HPD. VICTIM 1 was contacted and confirmed that he/she was the victim of fraud. VICTIM 1 advised that an individual identifying himself as CC1 told VICTIM 1 to mail $10,000 to the Hoboken FedEx Store.

8. On or about November 19, 2019, upon arrival at the Hoboken FedEx Store, law enforcement officers from HPD counted the USC and confirmed that the suspicious package contained approximately $10,000 in

USC.

9. Hoboken FedEx Store management advised law enforcement officers from HPD that on or about November 16, 2019, the store was contacted by C.F. who requested that a hold be placed on a package identified by FedEx tracking number 778065962739. C.R. explained that a family member (VICTIM 2 from West Chicago, Illinois) was the victim of fraud and had sent $15,000 in USC to the name of Co-Conspirator 3 (hereinafter "CC3"). Hoboken FedEx Store management was unable to hold the package as it had already been claimed and signed for. The Hoboken FedEx Store captured video footage of CC3 signing for the package on or about November 16, 2019.

10. Hoboken FedEx Store management further advised that the Hoboken FedEx Store was contacted on November 19, 2019, by a police officer from Tulsa, Oklahoma concerning a package, identified by FedEx tracking number 778060359046, that was sent by VICTIM 3 from Tulsa, Oklahoma. VICTIM 3 notified the Tulsa Police Department that he/she was the victim of fraud and indicated that $11,000 in USC was sent to "A. Mitra" at the Hoboken FedEx Store. According to Hoboken FedEx Store records, on November 16, 2019, the package was signed for by "A. Mitra." The Hoboken FedEx Store captured video footage of defendant ARUSHOBIKE MITRA signing for the package.

11. In addition to the above-described packages, HPD received a complaint from C.M. who indicated that her mother, (VICTIM 4 from Goodyear, Arizona), received an e-mail that indicated $24,000 was mistakenly deposited into her bank account and to call the listed number for more information. VICTIM 4 was subsequently instructed to send $10,000 in USC via FedEx to the Hoboken FedEx Store. The package was to be addressed to "A. Mitra." The package was identified by FedEx tracking number 778059631243 and was picked up on November 16, 2019. It was later determined that VICTIM 4 had sent a second package, identified by FedEx tracking number 778058453430, which was scheduled to be delivered on November 22, 2019. The second package was held at the FedEx location in Avandale, Arizona.

12. Hoboken FedEx Store management identified an additional package that was shipped to the Hoboken FedEx Store, FedEx tracking number 778065962739, by VICTIM 5 of Glendale Heights, Illinois. The package was signed for by CC3 on November 16, 2019 and contained approximately $15,000 in USC.

13. On or about November 20, 2019, HPD was contacted by Hoboken FedEx Store management concerning two additional suspicious packages, which were identified by FedEx tracking numbers 778153825752 and 778160115342. Both packages were addressed to defendant ARUSHOBIKE

MITRA. While law enforcement officers from HPD were at the Hoboken FedEx Store, defendant ARUSHOBIKE MITRA entered the store to pick up the packages. Law enforcement officers approached defendant ARUSHOBIKE MITRA and requested to see his identification. When questioned regarding the contents of the packages, defendant ARUSHOBIKE MITRA alleged that he did not know, but believed the packages contained documents. Defendant ARUSHOBIKE MITRA further alleged that he was sent to retrieve the packages by his friend. Defendant ARUSHOBIKE MITRA provide HPD consent to open the packages.

14. The package identified by FedEx tracking number 778153825752 was shipped by VICTIM 6 of Long Neck, Delaware. The package was determined to contain an alarm clock filled with USC wrapped in aluminum foil. The package contained approximately $9,800 in USC.

15. On or about November 20, 2019, law enforcement officers from HPD were able to contact VICTIM 6 who advised the he/she was contacted by two males who alleged that VICTIM 6 was involved in a lawsuit and needed to pay a certain amount of money or VICTIM 6's property would be seized. VICTIM 6 allowed the callers remote access to his/her computer while VICTIM 6 was logged in to online banking. VICTIM 6 was then directed to go to the bank and withdraw $10,000. Thereafter, VICTIM 6 was instructed to wrap the money inside aluminum foil and place it inside an empty alarm clock. VICTIM 6 was further directed to ship the money overnight to defendant ARUSHOBIKE MITRA at the Hoboken FedEx Store.

16. The package identified by FedEx tracking number 778160115342 was determined to contain two manila envelopes. Inside the envelopes were magazines filled with USC. The package contained a total of approximately $30,000 in USC. The sender was identified as VICTIM 7 of Dana Point, California.

17. Further investigation by the Social Security Administration, Office of the Inspector General revealed that on or about July 13, 2019, VICTIM 8 of Schaumburg, Illinois contacted the Schaumburg Police Department and reported being a victim of a phone scam. According to VICTIM 8, he/she received a telephone call from an individual claiming to be from the AT&T Fraud Department. The AT&T caller alleged that a BMO Harris Bank employee had gained access to VICTIM 8's BMO Harris bank account and was attempting to steal money from VICTIM 8's account. The individual who purported to be from the AT&T Fraud Department advised that he could provide assistance if VICTIM 8 provided him access to VICTIM 8's computer. VICTIM 8 provided remote access to their computer while pulling up their BMO Harris banking information for an account ending in 6710. The caller instructed VICTIM 8 to wire money to a different account so that the hacker

could be tracked and caught. VICTIM 8 was provided specific instructions as to the routing numbers and account numbers so as to wire the money. As a result, VICTIM 8 caused the following wire transfers from VICTIM 8's BMO Harris bank account:

DATE	AMOUNT	BENEFICIARY	BENEFICIARY BANK
July 2, 2019	$20,000	M.D.H	TD Bank Account Ending 6748
July 3, 2019	$25,000	CC2	Citibank Account Ending 7047
July 5, 2019	$25,000	A.Mitra (defendant ARUSHOBIKE MITRA)	HSBC Account Ending 0806

VICTIM 8 was further instructed to purchase gift cards. VICTIM 8 purchased approximately 31 gift cards from discount department stores to include Target and WalMart, which totaled approximately $12,600. VICTIM 8 provided the gift card numbers and related information to the caller.

18. On February 11, 2020, U.S. Postal Inspectors spoke with VICTIM 9 from Beaumont, Texas, who received an automated message from AT&T concerning an incorrect refund. Upon selecting Option 1 on the automated telephone call, VICTIM 9 was transferred to a representative who identified himself as an AT&T employee. VICTIM 9 was told that a refund was mistakenly deposited into VICTIM 9's bank account and that AT&T needed to recover the money. The caller coerced VICTIM 9 to provide remote access to VICTIM 9's computer. The caller further coerced VICTIM 9 to log into his/her bank accounts. VICTIM 9 was made to believe that he/she needed to refund AT&T approximately $28,000. VICTIM 9 wired the money as instructed from VICTIM 9's Capital One, N.A. account ending in 9973. VICTIM 9 wired the requested money; however, VICTIM 9 was advised that the wire was never processed. VICTIM 9 subsequently completed a second wire transfer in the same amount. A review of financial records confirmed the following wire transfers completed by VICTIM 9:

DATE	AMOUNT	BENEFICIARY	BENEFICIARY BANK
June 18, 2019	$28,000	M.A.	BB&T Bank Account Ending 3915
July 28, 2019	$28,000[1]	G. Mitra (defendant GARBITA MITRA)	JPMorgan Chase Account Ending 2357

19. On or about July 25, 2019, VICTIM 10 from San Antonio, Texas , notified Bank of America that he/she received a telephone call from an unidentified caller who claimed to be from Microsoft. During the conversation, VICTIM 10 was coerced into providing the caller with remote access to VICTIM 10's computer. The following unauthorized transactions from VICTIM 10's bank accounts resulted from the remote computer access:

DATE	AMOUNT	BENEFICIARY	BENEFICIARY BANK
July 15, 2019	$18,500	Defendant ARUSHOBIKE MITRA	HSBC Bank Account Ending 0806
July 16, 2019	$18,100	Defendant GARBITA MITRA	TD Bank Account Ending 7691

20. Further investigation by Social Security Administration, Office of the Inspector General revealed the following:

A. On or about July 3, 2019, VICTIM 11 of Portland, Oregon reported that he/she had received telephone calls from individuals who claimed that they were with Social Security. The callers represented that VICTIM 11 had been charged with 25 counts of social security fraud and that all of VICTIM 11's funds were going to be frozen and liquidated from her Advantis Federal Credit Union account. VICTIM 11 was instructed to withdraw and send all of the funds in her account so the funds could be verified. The callers also advised VICTIM 10 that there was a warrant for her arrest and that if she told the police or the bank she would be sued for damages. VICTIM 11

[1] The $28,000 wire transfer completed on July 28, 2019 was returned to VICTIM 9.

withdrew approximately $45,000, wrapped the USC in heavy aluminum foil, and sent the USC via UPS. VICTIM 11 was further instructed to secure a teller check in the amount of $32,300 payable to "Officer Garbita Mitra, Treasury Department." After securing the teller check, bank personnel discovered that VICTIM 11 was the victim of fraud and were able to stop VICTIM 11 from sending the teller check.

B. On or about June 27, 2019, VICTIM 12 of Calabash, NC reported that he/she had received telephone calls from individuals who claimed that they were with a computer protection program from whom VICTIM 12 had purchased a lifetime protection program from two years ago. The caller indicated that the company was going out of business and they were giving customers who purchased lifetime packages a $2,000 refund. The caller convinced VICTIM 12 to grant him access to VICTIM 12's computer and VICTIM 12 saw that the caller put $20,000 instead of $2,000. The caller indicated that in order to fix the mistake, VICTIM 12 needed to mail an $18,000 cashier's check to "Garbita Mita" at 250 E. Houston St, NYC, New York. After VICTIM 12 mailed the cashier's check as instructed, he/she discovered that the $20,000 deposited into VICTIM 12's checking account was actually a transfer from VICTIM 12's savings account.

C. On or about June 28, 2019, VICTIM 13 from Fort Wayne, Indiana, was also the victim of a computer tech remote access refund scam. Similar to other victims, VICTIM 13 was made to believe an overpayment refund was issued in the amount $17,500 into VICTIM 14's checking account. VICTIM 13 was instructed to return the funds via wire transfer to a Citibank Account ending in 4175, in the name of "Garbita Mitra", and an address of 786 Newark Ave., 3rd Floor, Jersey City, New Jersey. After sending the wire, VICTIM 13 discovered that the alleged "overpayment refund" was actually a transfer from VICTIM 13's own bank accounts.

21. On November 20, 2019, law enforcement officers from HPD arrested and charged defendant ARUSHOBIKE MITRA with Conspiracy to Commit Theft by Deception and Theft. Law enforcement officers determined that defendant ARUSHOBIKE MITRA was staying at 2672 Kennedy Blvd, Apt. 402, Jersey City, NJ 07030. Defendant ARUSHOBIKE MITRA was residing in the same apartment with CC1, CC2, CC3, and others.

22. After waiving his Miranda Rights, defendant ARUSHOBIKE MITRA advised, substance and in part, that he picked up packages for his friend, CC3, and delivered the packages to CC3 at his residence located at 2672 Kennedy

Blvd, Apt. 402, Jersey City, NJ 07030. Defendant ARUSHOBIKE MITRA confirmed that many of the packages were in his name and that he had picked up other packages at the direction of CC3. Defendant ARUSHOBIKE MITRA was unable to provide specific details about the other packages he picked up, but did advise that he took rideshare services to retrieve the packages. When presented with surveillance video from the Hoboken FedEx Store from November 2019, defendant ARUSHOBIKE MITRA identified the two individuals in the video picking up a package as CC3 and CC1.

23. Defendant ARUSHOBIKE MITRA also provided law enforcement officers from HPD with consent to search his cellular telephone. A review of the telephone revealed that defendant CC3 sent a text message to defendant ARUSHOBIKE MITRA and asked what the police were asking him. CC3 also provided defendant ARUSHOBIKE MITRA with an alibi to tell the police about the packages.

24. On or about November 20, 2019, following the arrest of defendant ARUSHOBIKE MITRA, law enforcement officers from HPD were contacted by the Hoboken FedEx Store concerning another suspicious package addressed to "Mitra Arushobike." The package was determined to contain a PVC pipe filled with $10,000 in USC wrapped in aluminum foil. The package was sent by VICTIM 14 from Mankato, Minnesota.

25. On or about November 22, 2019, law enforcement officers from HPD arrested CC3 at his apartment in Jersey City, New Jersey. CC3 was charged with Conspiracy to Commit Theft by Deception, Theft, and related charges. At the time of his arrest, CC3 had three cellular telephones in his possession. The cellular telephones were seized by law enforcement. CC3 provided law enforcement consent to search his cellular telephones.

26. After waiving his Miranda Rights, CC3 advised, in substance and in part, that he was not aware any packages contained USC and that he only picked up one package with CC1 during November 2019 at the Hoboken FedEx Store. CC3 further advised, in substance and in part, that he was aware of a scheme where calls are made from the Kolkata region of India to target elderly people and scam them to send money to certain locations where defendants ARUSHOBIKE MITRA, CC1, and CC3 would pick up the packages. CC3 indicated that CC3, CC1, and defendant ARUSHOBIKE MITRA received information as to when and where the packages would arrive.

27. On or about November 22, 2019, a search warrant was authorized by the Hudson County Superior Court, Jersey City, NJ, and a search was executed at the property located at 2672 John F. Kennedy Blvd., Apt. 402, Jersey City, NJ 07306. Law enforcement officers from HPD recovered a ledger composition book, empty FedEx and UPS boxes, a money counter, bank

documents, a box containing foil and Discover financial documents in the name of C.P., color coded money bands, and electronic devices, among other items. The ledger composition book was determined to be in the name of CC2 and listed financial transactions and tracking numbers.

28. On November 22, 2019, HPD arrested CC2 and charged him with Conspiracy to Commit Theft by Deception and Money Laundering. After waiving his Miranda Rights, CC2 advised, in substance and in part, that he moved into the Jersey City apartment at 2672 Kennedy Blvd., Apt. 402, Jersey City, NJ and met CC3 and defendant ARUSHOBIKE MITRA. CC2 observed CC3 and defendant ARUSHOBIKE MITRA with large amounts of USC every few days. CC2 also observed multiple FedEx and UPS boxes in the apartment. CC2 further advised, in substance and in part, that approximately two months prior to his arrest he was approached by defendant ARUSHOBIKE MITRA about picking up a box from a FedEx store in New York City. Defendant ARUSHOBIKE MITRA offered to pay CC2 $100 to retrieve the package. Defendant ARUSHOBIKE MITRA explained that the package contained a large amount of USC. CC2 was approached by defendant ARUSHOBIKE MITRA approximately five times and picked up packages in Jersey City, NJ, and New York City. CC2 always provided the packages to defendant ARUSHOBIKE MITRA or CC3.

29. Law enforcement officers completed a cursory consent search of CC3's cellular telephones and identified the following items, which further substantiate CC3's involvement in the scheme:

a. An image of a Bank of America Funds Transfer Request Authorizations (FTRA) dated September 13, 2019, from the Bank of America account of J.J. of Manhattan Beach, California to the SunTrust Bank account of CC3 ending in 9922. The transfer amount was $299,400.

b. Multiple videos of CC3 opening packages and counting USC.

c. A video showing remote access to the USAA account of an individual named Michael with an account/member number ending in 4367.

d. Over 100 UPS and FedEx tracking numbers.

e. Images of packages some of which were addressed to CC1, CC3, and CC3.

f. Bank account numbers, user names, passwords, account balances, identification documents, driver licenses, wire transfer receipts, and other financial related documents.